FOR610.1: Malware Analysis Fundamentals

• Assembling a toolkit for effective malware analysis
• Examining static properties of suspicious programs
• Performing behavioral analysis of malicious Windows executables
• Performing dynamic code analysis of malicious Windows executables
• Interacting with malware in a lab to derive additional behavioral characteristics

FOR610.2: Reversing Malicious Code

• Understanding core x86 assembly concepts to perform malicious code analysis
• Identifying key assembly logic structures with a disassembler
• Following program control flow to understand decision points during execution
• Recognizing common malware characteristics at the Windows API level (registry manipulation, keylogging, HTTP communications, droppers)
• Extending assembly knowledge to include x64 code analysis

FOR610.3: Malicious Web and Document Files

• Interacting with malicious websites to assess the nature of their threats
• De-obfuscating malicious JavaScript using debuggers and interpreters
• Analyzing suspicious PDF files
• Examining malicious Microsoft Office documents, including files with macros
• Analyzing malicious RTF document files

FOR610.4: In-Depth Malware Analysis

• Recognizing packed malware
• Getting started with unpacking
• Using debuggers for dumping packed malware from memory
• Examing obfuscated PowerShell scripts
• Analyzing multi-technology and fileless malware
• Code injection and API hooking
• Using memory forensics for malware analysis

FOR610.5: Examining Self-Defending Malware

• How malware detects debuggers and protects embedded data
• Unpacking malicious software that employs process hollowing
• Bypassing the attempts by malware to detect and evade the analysis toolkit
• Handling code misdirection techniques, including SEH and TLS Callbacks
• Unpacking malicious executable by anticipating the packer's actions

FOR610.6: Malware Analysis Tournament

- Behavioral malware analysis
- Dynamic malware analysis (using a debugger)
- Static malware analysis (using a disassembler)
- JavaScript deobfuscation
- PDF document analysis
- Microsoft Office document analysis
- Memory analysis